

PATENT ABSTRACTS OF JAPAN

(11)Publication number :

07-107083

(43)Date of publication of application : 21.04.1995

(51)Int.Cl.

H04L 9/00

H04L 9/10

H04L 9/12

H04L 12/28

(21)Application number : 05-250851

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 06.10.1993

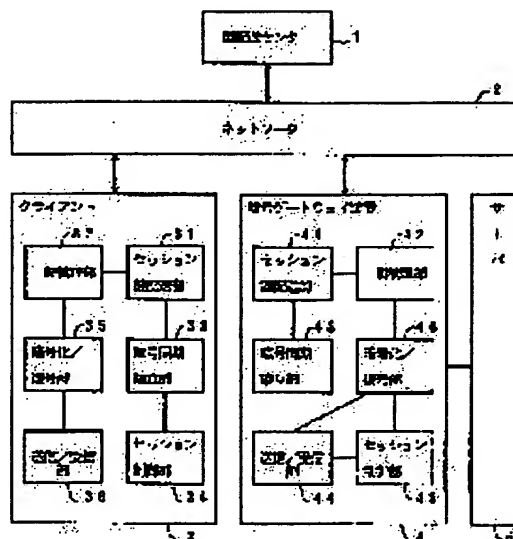
(72)Inventor : YAMAGUCHI TOSHIKAZU

(54) CIPHER COMMUNICATION SYSTEM

(57)Abstract:

PURPOSE: To eliminate the need of altering existing application and hardwares and to improve cost effectiveness by sharing a common key among a client, a cipher and a cipher gateway and performing cipher communication using the session key.

CONSTITUTION: The client 3 establishes a session with a cipher gateway device 4 before establishing the session with a server 5 and requests the cipher communication to the device 4. When a communication request is detected, the device 4 receives the session key ciphered by the respective cryptographic keys of the client 3 and the device 4 from a key delivery center 1. Then, the device 4 transmits the session key received from the center 1 to the client 3 and the client 3 receives the session key. The client 3 deciphers the session key by using the cryptographic key of its own and obtains the session key. Thus, the same session key is provided in the client 3 and the device 4. Then, cipher synchronization establishment parts 33 and 34 establish cipher synchronization between the client 3 and the device 4.



LEGAL STATUS

[Date of request for examination]

23.10.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3263878

[Date of registration]

28.12.2001

[Number of appeal against examiner's decision]

(19) 日本国特許庁 (JP)

(12) 特許公報 (B 2)

(11) 特許番号

特許第 3 2 6 3 8 7 8 号

(P 3 2 6 3 8 7 8)

(45) 発行日 平成14年3月11日 (2002. 3. 11)

(24) 登録日 平成13年12月28日 (2001. 12. 28)

(51) Int. Cl.⁷

識別記号

F I

H 0 4 L 9/08

H 0 4 L 9/00 6 0 1 B

12/28

11/00 3 1 0 Z

請求項の数 3

(全 1 4 頁)

(21) 出願番号 特願平5-250851

(22) 出願日 平成5年10月6日 (1993. 10. 6)

(65) 公開番号 特開平7-107083

(43) 公開日 平成7年4月21日 (1995. 4. 21)

審査請求日 平成10年10月23日 (1998. 10. 23)

(73) 特許権者 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 山口 利和

東京都千代田区内幸町1丁目1番6号 日本

電信電話株式会社内

(74) 代理人 100070150

弁理士 伊東 忠彦

審査官 青木 重徳

最終頁に続く

(54) 【発明の名称】 暗号通信システム

1

(57) 【特許請求の範囲】

【請求項 1】 ネットワークを介して複数のクライアントならびにサーバが鍵配送センタに接続され、該鍵配送センタが生成したセッション鍵を該ネットワークを介して入手することにより、任意のクライアント・サーバ間でセッションを確立して暗号通信を行う通信システムにおいて、

該サーバと該ネットワークの間に位置し、該クライアントが該サーバとの通信用セッションの確立に先立って出力する暗号通信要求を受信して、該鍵配送センタからセッション鍵を取得し、該クライアントに配送するゲートウェイセッション鍵配送手段と、該鍵配送手段で取得したセッション鍵によりパケットを暗号化または復号する第1の暗号化／復号手段とを含む暗号ゲートウェイ装置と、

2

該サーバとの通信用セッションの確立に先立ち、該暗号ゲートウェイ装置に暗号通信を要求し、該暗号ゲートウェイ装置からセッション鍵を取得するセッション鍵取得手段と、該セッション鍵取得手段により得た該セッション鍵を保持するセッション鍵保持手段と、該暗号ゲートウェイ装置との暗号同期を確立する同期確立手段と、該同期確立手段による同期確立を契機としてサーバとのセッションを確立する第1のセッション確立手段と暗号同期が確立し、かつセッション確立後、パケットを暗号化または復号する第2の暗号化／復号手段とを含むクライアントと、

該クライアント・該サーバ間のセッション確立に先立って、該クライアントからの暗号通信要求に対して、該鍵配送センタから当該セッションで使用するセッション鍵を該暗号ゲートウェイ装置が取得し、該クライアントに

配送し、該クライアント・該ゲートウェイ装置間で共通のセッション鍵を共有することを特徴とする暗号通信システム。

【請求項 2】 前記クライアントは、前記サーバとの通信用セッションの確立に先立ち、前記ネットワークを介して前記鍵配送センタからセッション鍵を取得すると共に、前記暗号ゲートウェイ装置に配送するクライアントセッション鍵配送手段を含み、

前記暗号ゲートウェイ装置は、該クライアントからの暗号通信要求と該クライアントセッション鍵配送手段により配送された該セッション鍵を受信するセッション鍵受信手段を含む請求項 1 記載の暗号通信システム。

【請求項 3】 前記クライアントは、前記サーバとの通信用セッションの確立に先立ち、前記暗号ゲートウェイ装置に対して暗号通信を要求するために前記暗号ゲートウェイ装置の特定ポートとセッションを確立する第 2 のセッション同期確立手段を含み、
前記暗号ゲートウェイ装置は、該第 2 のセッション同期確立手段による前記クライアントからの特定ポートへのセッション確立を契機として、前記鍵配送センタからセッション鍵を取得し、前記クライアントに配送する第 2 のゲートウェイセッション鍵配送手段を含む請求項 1 記載の暗号通信システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、暗号通信システムに係り、特に、ネットワークを介して複数のクライアントとサーバが鍵配送センタに接続され、その中の任意のクライアントとサーバが鍵配送センタが生成したセッション鍵を入手し、この鍵を用いてセッションを確立し、共通鍵暗号アルゴリズムを用いてクライアントとサーバ間で暗号通信を行う暗号通信システムに関する。

【0002】

【従来の技術】 図 10 は、従来の暗号通信システムの構成を示す。同図に示す従来の暗号通信システムは、ネットワーク 2 を介して、複数のクライアント 3₁～3₃、及びサーバ 5 が鍵配送センタ 1 に接続され、鍵配送センタ 1 が生成したセッション鍵をクライアント 3 またはサーバ 5 が入手する。

【0003】 図 11 は、従来の暗号通信システムを説明するための図である。同図 (A) は、鍵配送センタ 1 にセッション鍵を要求する場合に、クライアント 3 からアプリケーションプログラムを用いて要求する場合を示し、同図 (B) は、サーバ 5 からアプリケーションプログラムを用いて要求する場合を示す。このように、クライアント 3 またはサーバ 5 がアプリケーションプログラムを用いて通信に使用するセッション鍵を取得する。このセッション鍵をクライアント 3 とサーバ 5 間で共有し、以降の通信パケットをこのセッション鍵を用いて暗号化あるいは、復号し、暗号通信を行う。

【0004】 このように、従来の暗号通信システムは、広い地域に分散した事業所等の特定の端末間で暗号通信を行う LAN 等に効果的に利用できるものである。

【0005】

【発明が解決しようとする課題】 しなしながら、上記従来の方式では、暗号通信に先立ち、クライアントあるいはサーバ上で走行するアプリケーションプログラムが鍵配送センタとセッションを確立し、鍵配送センタからセッション鍵を取得し、かつ通信相手のサーバあるいはクライアントのアプリケーションに同じセッション鍵を送信する処理が必要となる。

【0006】 一方、コネクション型のネットワークを介して、クライアント・サーバ間で通信を行う通信プログラムの数は膨大であり、これらを暗号通信対応に変更する場合には、個別にアプリケーションプログラムやクライアントあるいはサーバのハードウェアを改造する必要があり、改造規模や工数が大きくなり、これに伴って、開発費も大きくなるという問題がある。

【0007】 本発明は、上記の点に鑑みなされたもので、上記従来の問題点を解決し、既存のアプリケーションプログラムやハードウェアに影響を与えることなく暗号通信を行うことができる暗号通信システムを提供することを目的とする。

【0008】

【課題を解決するための手段】 図 1 は、本発明の原理構成図である。

【0009】 本発明は、ネットワーク 2 を介して複数のクライアント 3 ならびにサーバ 5 が鍵配送センタ 1 に接続され、鍵配送センタ 1 が生成したセッション鍵をネットワーク 2 を介して入手することにより、任意のクライアント・サーバ間でセッションを確立して暗号通信を行う通信システムにおいて、サーバ 5 とネットワーク 2 の間に位置し、クライアント 3 がサーバ 5 との通信用セッションの確立に先立って出力する暗号通信要求を受信して、鍵配送センタ 1 からセッション鍵を取得し、クライアント 3 に配送する第 1 のゲートウェイセッション鍵配送手段 107 と、鍵配送手段 107 で取得したセッション鍵によりパケットを暗号化または復号する第 1 の暗号化／復号手段 110 とを含む暗号ゲートウェイ装置 4 と、サーバ 5 との通信用セッションの確立に先立ち、暗号ゲートウェイ装置 4 に暗号通信を要求し、暗号ゲートウェイ装置 4 からセッション鍵を取得するセッション鍵取得手段 101 と、セッション鍵取得手段 101 により得たセッション鍵を保持するセッション鍵保持手段 102 と、暗号ゲートウェイ装置 4 との暗号同期を確立する同期確立手段 103 と、同期確立手段 103 による同期確立を契機としてサーバ 5 とのセッションを確立する第 1 のセッション確立手段 104 と、暗号同期が確立し、かつセッション確立後パケットを暗号化または復号する第 2 の暗号化／復号手段 111 とを含むクライアント 3

と、クライアント・サーバ間のセッション確立に先立って、クライアント 3 からの暗号通信要求に対して、鍵配送センタ 1 から当該セッションで使用するセッション鍵を暗号ゲートウェイ装置 4 が取得し、クライアント 3 に配送し、クライアント・ゲートウェイ装置間で共通のセッション鍵を共有する。

【0010】また、本発明のクライアント 3 は、サーバ 5 との通信用セッションの確立に先立ち、ネットワーク 2 を介して鍵配送センタ 1 からセッション鍵を取得すると共に、暗号ゲートウェイ装置 4 に配送するクライアントセッション鍵配送手段 105 を含み、暗号ゲートウェイ装置 4 は、クライアント 3 からの暗号通信要求とクライアントセッション鍵配送手段 105 から配送されたセッション鍵を受信するセッション鍵受信手段 108 を含む。

【0011】また、本発明のクライアント 3 は、サーバとの通信用セッションの確立に先立ち、暗号ゲートウェイ装置 4 に対して暗号通信を要求するために暗号ゲートウェイ装置 4 の特定ポートとセッションを確立する第 2 のセッション確立手段 106 を含み、暗号ゲートウェイ装置 4 は、第 2 のセッション同期確立手段 106 によるクライアント 3 からの特定ポートへのセッションの確立を契機として、鍵配送センタ 1 からセッション鍵を取得し、クライアント 3 に配送する第 2 のゲートウェイセッション鍵配送手段 109 を含む。

【0012】

【作用】図 2 は、本発明のシーケンスの概要を示す図である。

【0013】本発明の暗号通信システムは、サーバとネットワークの間に位置する暗号ゲートウェイ装置は、クライアント・サーバ間のセッション確立に先立って、クライアントからの暗号通信要求（ステップ 1）に対して、鍵配送センタから当該セッションで使用するセッション鍵を取得し（ステップ 2）、クライアントに配送する（ステップ 3）。これによりクライアント・暗号ゲートウェイ装置間で同一のセッション鍵を共有する（ステップ 4）。クライアントは、暗号ゲートウェイとの暗号同期を確立し（ステップ 5）、暗号同期確立を契機としてサーバとのセッションを確立する（ステップ 6）。これ以降、クライアント・サーバ間のセッションが切断されるまでクライアント・ゲートウェイ装置間の暗号通信が可能である（ステップ 7）。

【0014】なお、ステップ 3 において、鍵配送センタ 1 よりセッション鍵を得る場合には、クライアントでもよく、クライアントがセッション鍵を取得すると暗号ゲートウェイ装置に配送することによりセッション鍵を共有することができる。

【0015】このように、本発明は、サーバにフロントエンドプロセッサとして暗号ゲートウェイ装置を接続し、この暗号ゲートウェイ装置がクライアントからの暗

号通信要求を契機として、鍵配送センタにアクセスし、セッション鍵を取得し、通信相手であるクライアントにも同じセッション鍵を配送し、セッション鍵を共有することにより、既存のアプリケーションプログラムやハードウェアの更新や、変更等を行わずに、暗号通信を行う。

【0016】

【実施例】以下、図面と共に本発明の実施例を詳細に説明する。

【0017】図 3 は、本発明のシステム全体図である。

同図に示す通信システムは、ネットワーク 2 を介して鍵配送センタ 1 と複数のクライアント 3、暗号ゲートウェイ装置 4 が接続され、暗号ゲートウェイ装置 4 にサーバ 5 が接続されている。また、クライアント 3 のフロントエンドとして暗号ゲートウェイ装置 4 が接続されることも考えられるが、本実施例では、暗号ゲートウェイ装置 4 は、サーバのフロントエンドとして接続されていることを前提とする。

【0018】以下、コネクション型のプロトコルを使用してパケット交換網を介して、通信を行う TCP/IP・LAN (Transmission Control Protocol, Internet Protocol, Local area network) を例にとり、詳細に説明する。

【0019】図 4 は、本発明の一実施例のシステム構成を示す。同図における通信システムは、鍵配送センタ 1、ネットワーク 2、クライアント 3、暗号ゲートウェイ装置 4 及びサーバ 5 より構成される。

【0020】鍵配送センタ 1 は、セッション鍵を生成して、暗号ゲートウェイ装置 4 に送信する。ネットワーク 2 は、クライアント 3 とサーバ 5 間、鍵配送センタ 1 と暗号ゲートウェイ装置 4 間、クライアント 3 と暗号ゲートウェイ装置 4 間でセッションを確立し、通信を行う。クライアント 3 及びサーバ 5 は、パケットのやり取りを行うことにより通信する。暗号ゲートウェイ装置 4 は、クライアント 3 とサーバ 5 間でやりとりするパケットを暗号化／復号する。

【0021】クライアント 3 は、暗号ゲートウェイ装置 4 に暗号通信を要求し、セッション鍵を取得するセッション鍵配送部 31 と、セッション鍵配送部 31 から受け取ったセッション鍵をセッション毎に管理する鍵管理部 32 と、クライアント 3 と暗号ゲートウェイ装置 4 間で暗号通信の同期を確立する暗号同期確立部 33 と、暗号同期確立部 33 から暗号同期確立完了信号を受け取ってサーバ 5 とのセッションを確立するセッション制御部 34 と、アプリケーション (AP) から受け取ったデータをサーバ 5 から受け取った暗号化されたパケットを復号する暗号化／復号部 35 と、ネットワーク 2 から (一) 暗号化されたパケットを受信 (送信) する送信／受信部 36 から構成される。

【0022】また、暗号ゲートウェイ装置 4 は、クライアント 3 からの暗号通信の要求を受け取り、鍵配送セン

タ 1 からセッション鍵を取得し、クライアント 3 に配送するセッション鍵配送部 4 1 と、セッション鍵配送部 4 1 から受け取ったセッション鍵をセッション毎に管理する鍵管理部 4 2 と、クライアント 3 と暗号ゲートウェイ装置 4 間で暗号通信の同期を確立する暗号同期確立部 4 3 と、クライアント 3 あるいは、サーバ 5 から (へ) パケットを受信 (送信) する送信/受信部 4 4 と、送信/受信部 4 4 から受け取ったパケットの IP ヘッダ及び TCP ヘッダから送信元 IP アドレス、送信元ポート番号、送信先 IP アドレス及び送信先ポート番号を取り出し、セッション番号を識別するセッション番号をキーとして鍵管理部 4 2 からセッション鍵を取得し、当該セッション鍵がサーバ 5 宛のパケットのものであれば、当該パケットを復号し、一方、当該セッション鍵がクライアント 3 宛のパケットであれば、当該パケットを暗号化する暗号化/復号部 4 6 から構成されている。

【0023】図 5 は、TCP/IP・LAN で使用するプロトコルを OSI の参照モデルに準拠して記述している。データリンクレイヤは、MAC (Media Access Control) プロトコル、ネットワークレイヤは、IP (Internet protocol)、トランスポートレイヤは TCP (Transmit Control Protocol) で実現されており、AP は、TCP レイヤ間でセッションを確立する。

【0024】図 6 は、TCP/IP・LAN に接続されたクライアント・サーバ間で通信する際に使用するパケット・フォーマットを示す。パケットは、MAC ヘッダ (MAC_H)、IP ヘッダ (IP_H) 及び TCP ヘッダ (TCP_H) からなるヘッダと、AP データ及びパケット全体のフレーム・チェック・シーケンス (FCS) から構成される。AP データに暗号をかけることにより、IP ルータを介したネットワークを使用して通信を行うことができる。なお、送信側の IP アドレス (IP ヘッダに規定) 及び、ポート番号 (TCP ヘッダに規定) と受信側の IP アドレス及びポート番号により、クライアント・サーバ間のセッションが一意に決定される。

【0025】暗号ゲートウェイ 4 のセッション識別部 4 5 は、送信/受信部 4 4 を介して受け取った図 6 に示す TCP ヘッダ、IC ヘッダから送信元 (クライアント) IP アドレス、送信元 (クライアント) のポート番号、送信先 IP アドレス、送信先ポート番号よりセッション番号を得る。セッション識別部 4 5 により得られたセッション番号に基づいて鍵管理部 4 2 から対応するセッション鍵を取得し、当該暗号ゲートウェイ装置 4 に接続されているサーバ宛のパケットであれば、暗号化/復号部 4 6 において取得したセッション鍵により復号し、サーバ 5 に対して非暗号化通信を行う。

【0026】図 7 は、TCP ヘッダのフォーマットを示す。同図において、“_” 部分は、本発明に直接関係がないため、ここでは説明を省略する。同図に示す TCP

ヘッダは 6 フレームからなり、第 1 フレームには、ソースポート番号 “SRC_PORT” 及び送信先ポート番号 “DST_PORT” が設定される。6 フレーム目にはオプションが設定され、7 フレーム目より任意のアプリケーションデータが設定される。

【0027】クライアント 3 からの暗号ゲートウェイ装置 4 に対する暗号通信の要求方法として、

①暗号ゲートウェイ装置 4 の特定ポート番号に対するセッション確立

②オプションを利用したメッセージ (暗号通信要求) の送信

③AP データを利用したメッセージ (暗号通信要求) の送信
がある。

【0028】図 8 は、本発明の一実施例の鍵配送手順を示すシーケンスチャートである。同図に基づいて以下にセッション鍵の配送の手順を説明する。なお、クライアント 3 及び暗号ゲートウェイ装置 4 の暗号鍵 K_{c1} 及び K_{sw} は、各装置のインストール時に各々装置内部に保持しており、外部からみることができない作りになっている。また、図 8 において、セッション鍵 $K_s = d K_{c1} (C_{c1}) : K_s$ は、暗号文 C_{c1} を暗号鍵 K_{c1} で復号した結果である。

【0029】手順 1) クライアント 3 は、サーバ 5 とのセッション確立に先立ち、暗号ゲートウェイ装置 4 とセッションを確立し (ステップ 101)、暗号ゲートウェイ装置 4 に暗号通信を要求する。この時、暗号ゲートウェイ装置 4 にクライアントの識別子 ID_{c1} を送信する (ステップ 102)。

【0030】手順 2) 暗号ゲートウェイ装置 4 は、暗号ゲートウェイ装置 4 からの通信要求を検出すると、鍵配送センタ 1 にアクセスし、鍵取得手順 (ステップ 103) (詳しくは図 9 に示す) により、クライアント 3 及び暗号ゲートウェイ装置 4 のそれぞれの暗号鍵 (K_{c1} 及び K_{sw}) で暗号化されたセッション鍵 (C_{c1} 及び C_{sw}) を鍵配送センタ 1 から受信する (ステップ 104)。

【0031】手順 3) セッション鍵 C_{sw} を暗号ゲートウェイ装置 4 の暗号鍵 K_{sw} で復号し、セッション鍵 K_s を取得する (ステップ 105)。セッション鍵 K_s はサーバ 5 とのセッションを切断するまで保持する。

【0032】手順 4) 暗号ゲートウェイ装置 4 は、クライアント 3 に鍵配送センタ 1 から受信したセッション鍵 C_{c1} を送信する (ステップ 106)。

【0033】手順 5) クライアント 3 は、暗号ゲートウェイ装置 4 からセッション鍵 C_{c1} を受信する (ステップ 107)。

【0034】手順 6) クライアント 3 は、自分の暗号鍵 K_{c1} を用いてセッション鍵 C_{c1} を復号し、セッション鍵 K_s を取得する (ステップ 108)。これにより、クライアント 3 と暗号ゲートウェイ装置 4 間で同じセッショ

ン鍵を持つこととなる。セッション鍵 K_s は、サーバ5とのセッションを切断するまで保持する。

【0035】手順7) 暗号同期確立部33、43がクライアント3と暗号ゲートウェイ装置4間で、暗号同期の確立を行う(ステップ109)。暗号同期確立が完了すると、クライアント3は、暗号ゲートウェイ装置4とのセッションを切断する(ステップ110)。なお、暗号同期の確立方法は、本発明とは直接関係がないので、説明は省略する。

【0036】手順8) クライアント3はサーバ5とセッションを確立する(ステップ111)。

【0037】手順9) 以降、共通のセッション鍵 K_s を用いてクライアント3と暗号ゲートウェイ装置4間の暗号通信が可能である(ステップ112)。

【0038】手順10) 暗号ゲートウェイ装置4は、クライアント3からサーバ5宛のパケットを受信し、該当するセッション鍵を使用してパケットを復号する(ステップ113)。この復号されたパケット(平文のパケット)をサーバ5に送信することにより、暗号ゲートウェイ装置4とサーバ5間で非暗号通信が可能である(ステップ114)。

【0039】また、サーバ5からクライアント3宛のパケットについては、暗号ゲートウェイ装置4において、暗号化され(ステップ113')、暗号化された暗号文にてクライアント3との暗号通信を行う。

【0040】次に、図9は、本発明の一実施例の暗号ゲートウェイ装置の鍵取得手順を示すシーケンスチャートである。

【0041】手順1) 暗号ゲートウェイ装置4のセッション鍵配送部41は、鍵配送センタ1にアクセスし、セッションを確立する(ステップ201)。

【0042】手順2) 暗号ゲートウェイ装置4は、鍵配送センタ1にクライアント3及び暗号ゲートウェイ装置4の識別子 ID_{c1} 及び ID_{gw} を送信する(ステップ202)。なお、識別子 ID_{c1} 及び ID_{gw} は装置を識別するための使用するIPアドレス或いは、MACアドレスである。

【0043】手順3) 鍵配送センタ1は、乱数を発生し、セッション鍵 K_s を生成する。さらにクライアント3及び暗号ゲートウェイ装置の暗号鍵 K_{c1} 及び K_{gw} を識別子 ID_{c1} 及び ID_{gw} に基づいて検索(或いは生成)する。ここで、暗号鍵 K_{c1} 及び K_{gw} の検索(或いは生成)する方法は、本発明の要点とは、直接関係がないので説明は省略する。

【0044】検索により暗号鍵 K_{c1} 及び K_{gw} を取得する場合には、暗号ゲートウェイ装置4の識別子及び暗号鍵を鍵配送センタ1のデータベースに登録する手段が必要であることは言うまでもない。

【0045】さらに、詳しい暗号鍵 K_{c1} 及び K_{gw} を生成する方法については、“小柳津、田中『UUIを利用し

た鍵配送方式』、信学技報、OFS92-31”を参照されたい。上記暗号鍵 K_{c1} 及び K_{gw} を用いて、セッション鍵 K_s を暗号化し、暗号文 C_{c1} 及び C_{gw} を生成する。図9において、 $C_{c1} = e_{K_{c1}}(K_s)$: C_{c1} は、平文 K_s を暗号鍵 K_{c1} で暗号化した結果である(ステップ203)。

【0046】手順4) 鍵配送センタ1は、暗号ゲートウェイ装置4に暗号文 C_{c1} 及び C_{gw} を送信する(ステップ204)。

【0047】手順5) 暗号ゲートウェイ装置4のセッション鍵管理部42は、暗号文 C_{c1} 及び C_{gw} を受信すると、鍵配送センタ1とのセッションを切断する(ステップ205)。

【0048】ここでは、暗号ゲートウェイ装置4と鍵配送センタ1間、セッションを確立して通信を行う例を説明したが、UDPプロトコルを使用するコネクションレス型の通信を使用してもよいし、また、他の通信手段を使用してもよいということはいくまでもない。

【0049】さらに、本発明は、鍵配送アルゴリズムを特定したものではない。従って、送信するデータの内容(ここでは、識別子 ID_{c1} 、 ID_{gw} 、 C_{c1} 、及び C_{gw})を変更すれば、相手端末の認証ができることについては“小柳津、田中：『UUIを利用した鍵配送方式』、信学技報、OFS92-31”を参照されたい。

【0050】なお、上記実施例では、暗号ゲートウェイ装置4が鍵配送センタ1よりセッション鍵を取得する場合について説明したが、クライアント3が同様に、鍵配送センタ1より取得し、暗号ゲートウェイ装置4にセッション鍵を配送してもよい。従って、上記図9に示す暗号ゲートウェイ装置4をクライアント3に読み替えればよい。

【0051】上記の実施例のように、ネットワーク2を介してクライアント・サーバ間の暗号通信を行う場合に、ネットワーク2とサーバ5間に暗号ゲートウェイ装置4を接続し、クライアント3とサーバ5間のセッション確立に先立って、クライアント3から暗号通信要求時に暗号ゲートウェイ装置4が鍵配送センタ1よりセッション鍵を取得し、クライアント3に配送する。これにより、クライアント3・暗号ゲートウェイ装置4間で同一のセッション鍵を共有する。これにより、クライアント3は、暗号ゲートウェイ装置4と暗号同期をとり、これを契機にクライアント3は、サーバ5とのセッションを確立する。この場合、サーバ5とゲートウェイ装置4の通信は、平文通信が行われる。このように、最終的にクライアント3とサーバ5のアプリケーションやハードウェアを変更することなしに、暗号通信が可能となる。

【0052】本発明は、上記実施例に限定されることなく、暗号ゲートウェイ装置4がサーバ5以外にクライアント3側に接続されてもよく、本発明の範囲を逸脱しない範囲で種々ネットワークを介した接続の変更及び鍵の

取得が可能である。

【0053】

【発明の効果】 上述のように、本発明によれば、クライアントとサーバの通信用セッションが確立する前に、サーバと接続されている暗号ゲートウェイ装置がクライアントからの暗号通信要求を受け付け、鍵配送センタにアクセスし、通信に使用するセッション鍵を取得し、通信相手であるクライアントにセッション鍵を配送し、クライアントと暗号ゲートウェイ間で、共通の鍵を共有し、このセッション鍵を用いて、暗号通信を行うため、従来のように既存のアプリケーションやハードウェアを改造する必要がなく、経済化を図ることができる。

【図面の簡単な説明】

【図1】 本発明の原理構成図である。

【図2】 本発明のシーケンスの概要を示す図である。

【図3】 本発明のシステム全体図である。

【図4】 本発明の一実施例のシステム構成図である。

【図5】 TCP/IP・LANで使用するプロトコルを示す図である。

【図6】 TCP/IP・LANのパケット・フォーマットを示す図である。

【図7】 TCPヘッダのフォーマットである。

【図8】 本発明の一実施例のシーケンスチャートである。

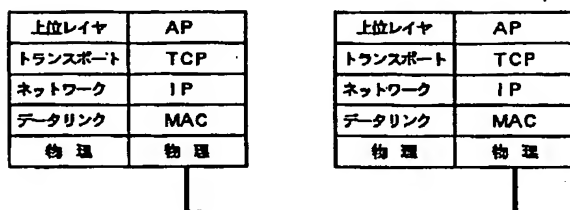
【図9】 本発明の一実施例の暗号ゲートウェイ装置の鍵取得手順を示すシーケンスチャートである。

【図10】 従来の暗号通信システムの構成図である。

【図11】 従来の暗号通信システムを説明するための図である。

【図5】

(TCP/IP・LANで使用するプロトコル)

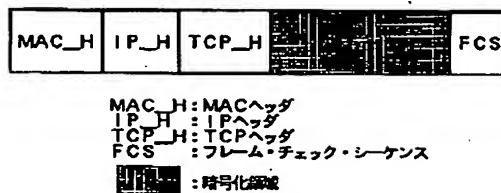


【符号の説明】

- 1 鍵配送センタ
- 2 ネットワーク
- 3 クライアント
- 4 暗号ゲートウェイ装置
- 5 サーバ
- 31 セッション鍵配送部
- 32 鍵管理部
- 33 暗号同期確立部
- 34 セッション制御部
- 35 暗号化／復号部
- 36 送信／受信部
- 41 セッション鍵配送部
- 42 鍵管理部
- 43 暗号同期確立部
- 44 送信／受信部
- 45 セッション識別部
- 46 暗号化／復号部
- 101 セッション鍵取得手段
- 102 セッション鍵保持手段
- 103 同期確立手段
- 104 第1のセッション確立手段
- 105 クライアントセッション鍵配送手段
- 106 第2のセッション確立手段
- 107 第1のゲートウェイセッション鍵配送手段
- 108 セッション鍵受信手段
- 109 第2のゲートウェイセッション鍵配送手段
- 110 第1の暗号化／復号手段
- 111 第2の暗号化／復号手段

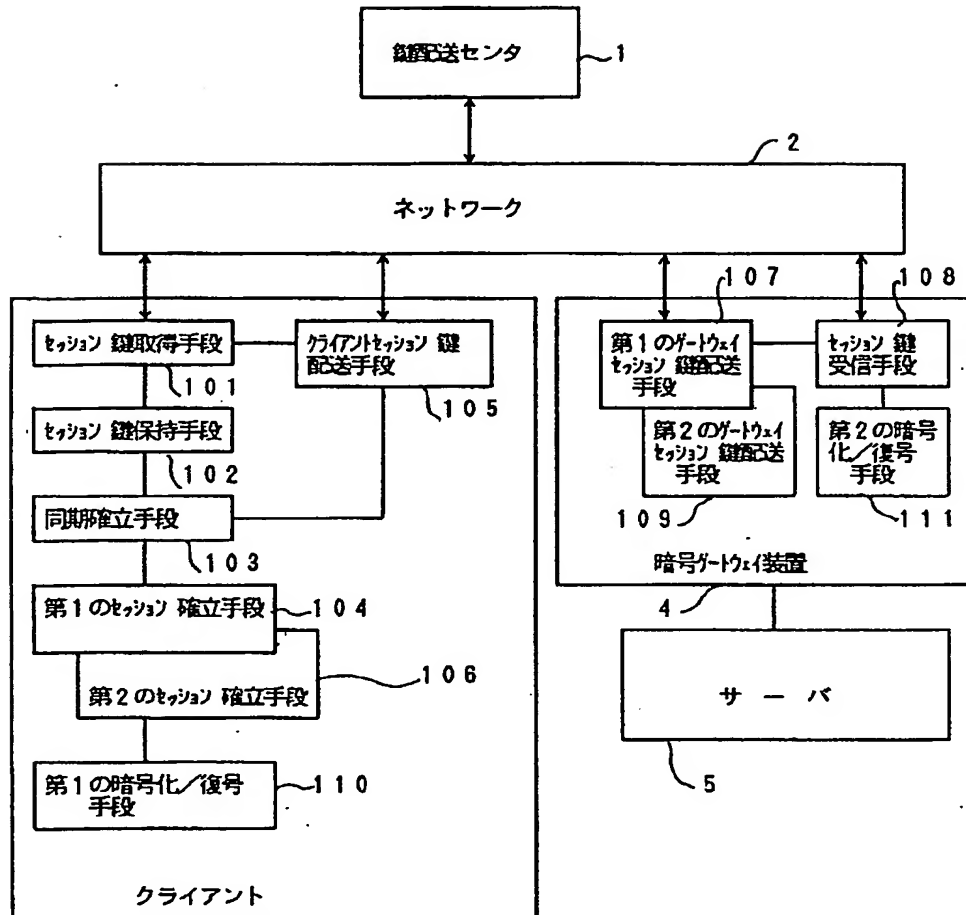
【図6】

(TCP/IP・LANのパケット・フォーマット)



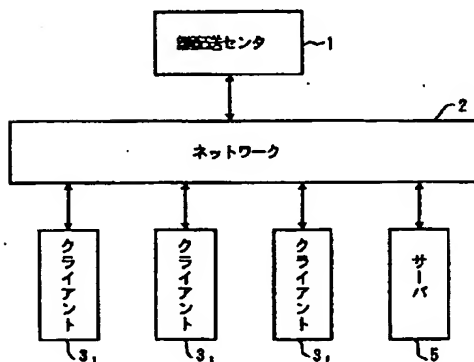
【図 1】

本発明の原理構成図



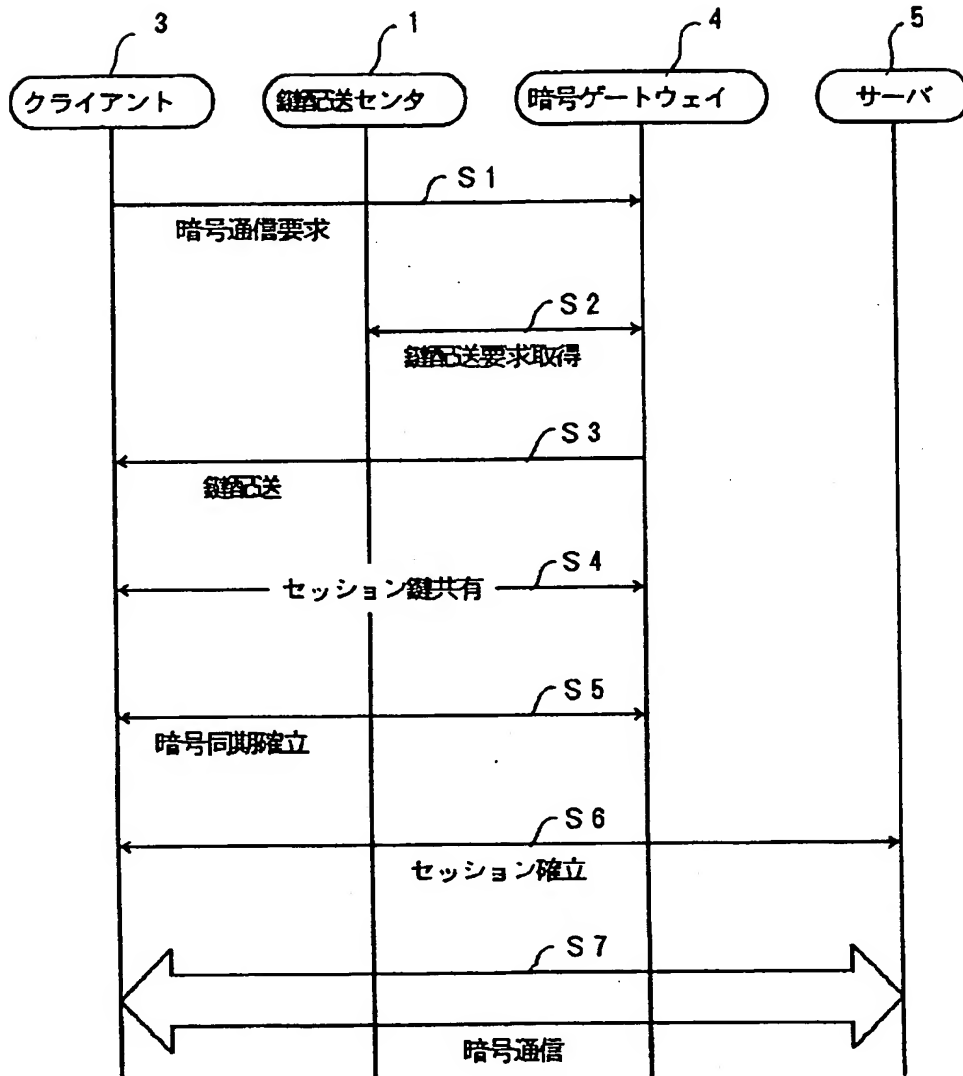
【図 10】

従来の暗号通信システムの構成図



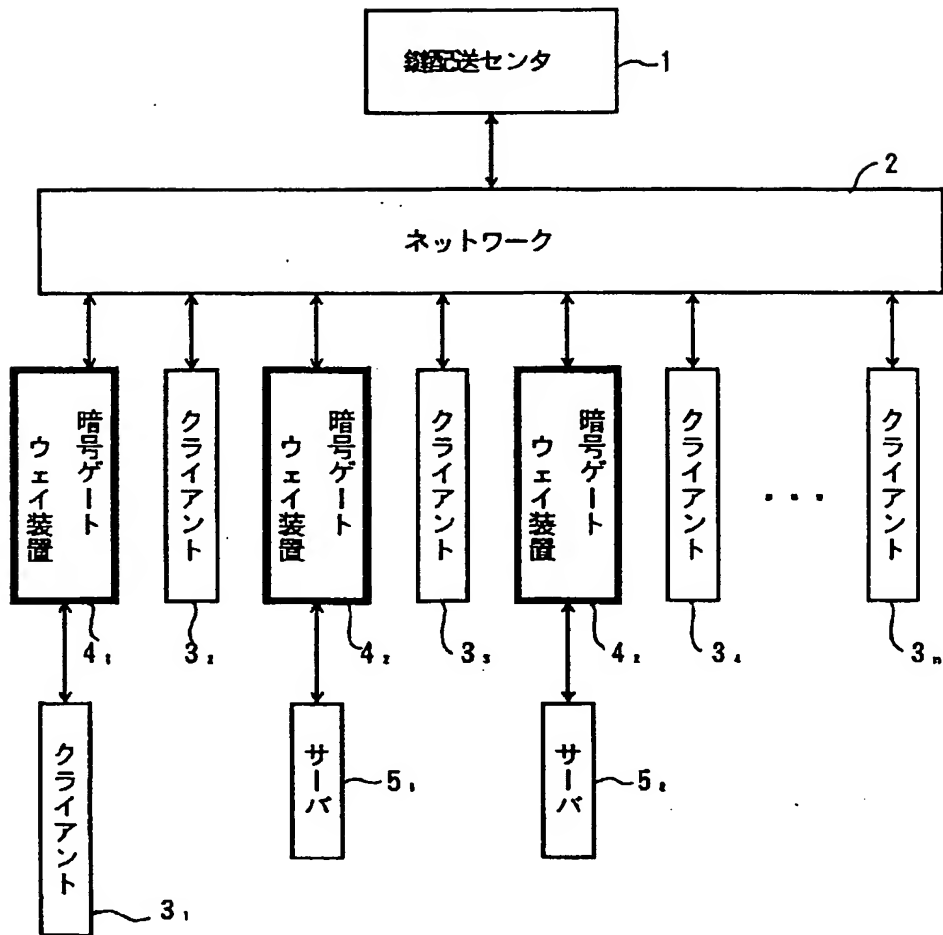
【図 2】

本発明のシーケンスの概要を示す図



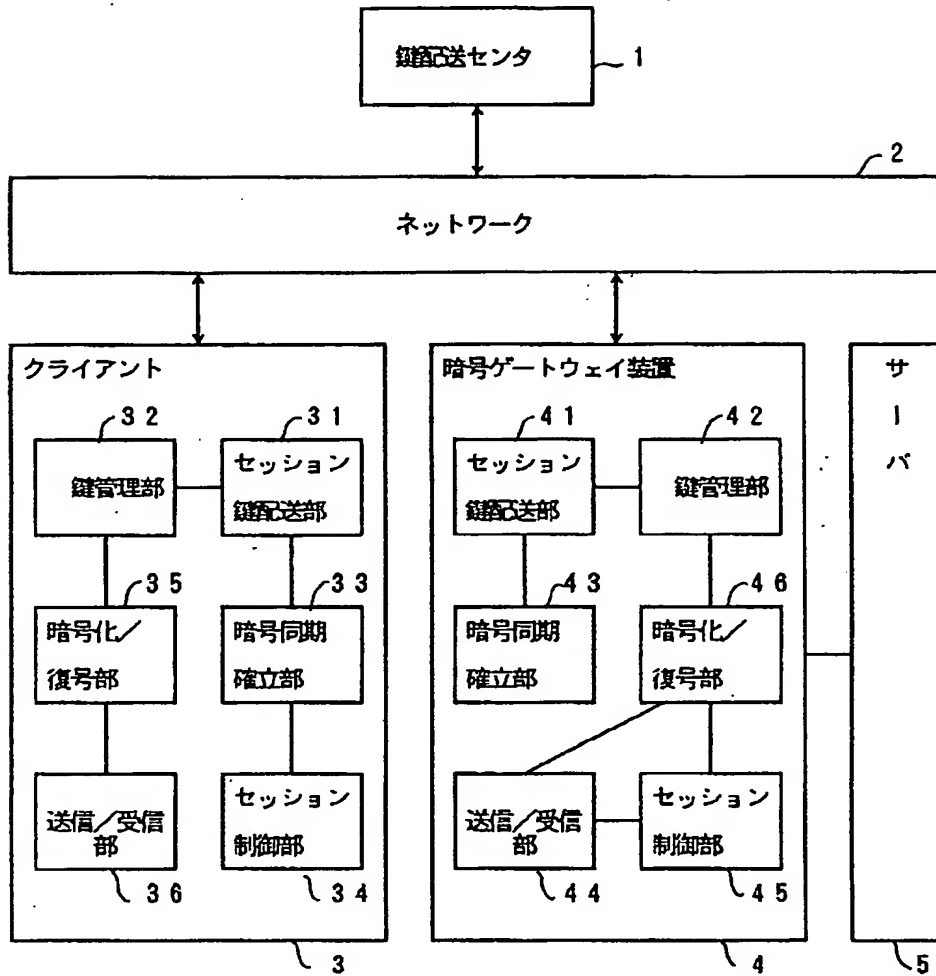
【図 3】

本発明のシステム全体図



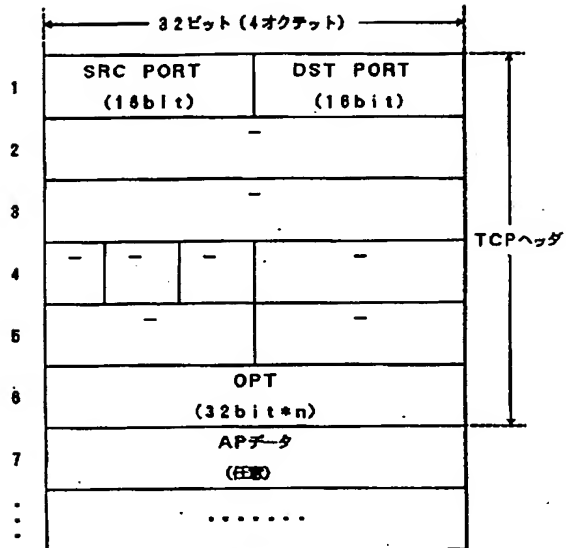
【図 4】

本発明の一実施例のシステム構成図



【図 7】

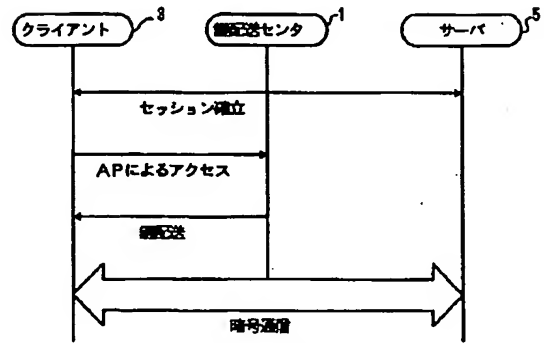
TCPヘッダのフォーマット



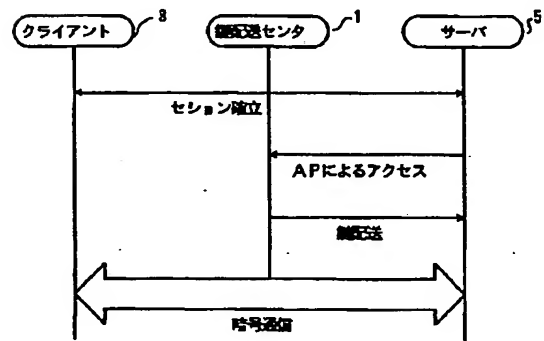
SRC PORT: ソース・ポート
 DST PORT: デスティネーション・ポート
 OPT: オプション

【図 11】

従来の暗号通信システムを説明するための図



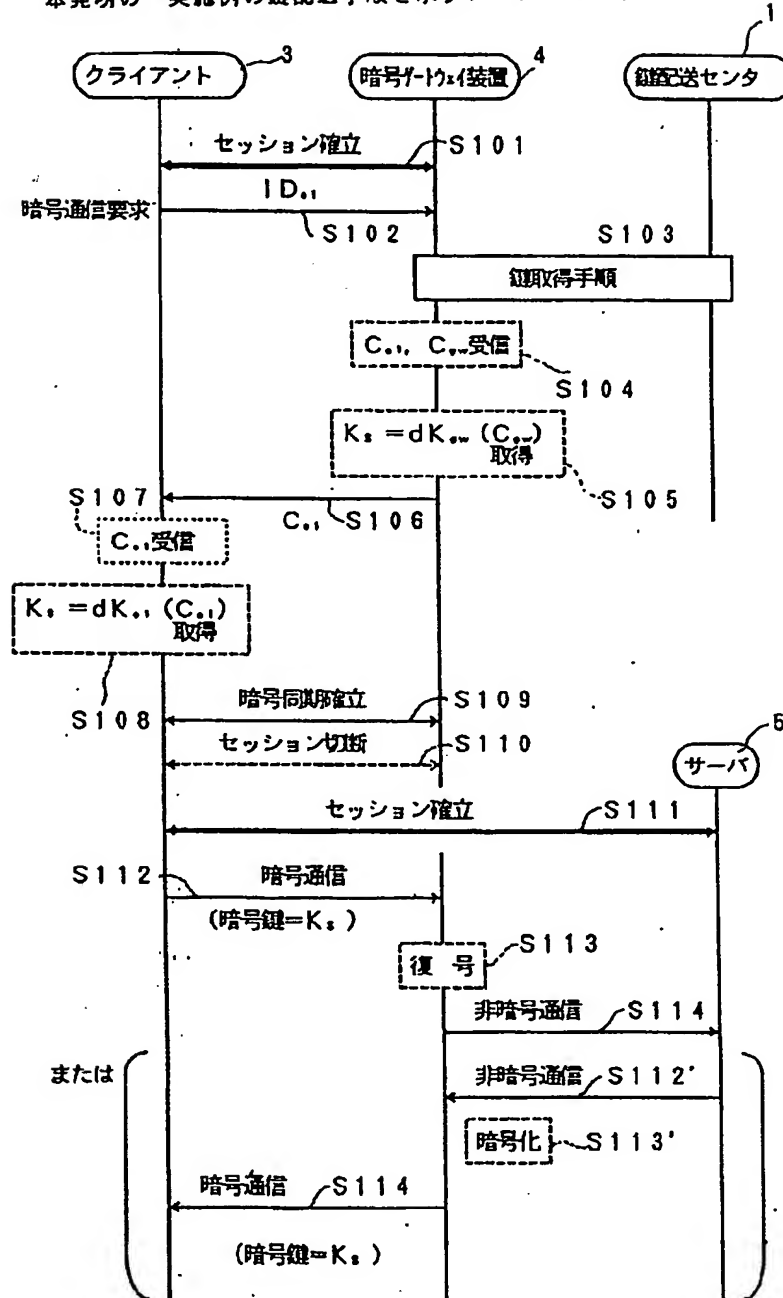
(A)



(B)

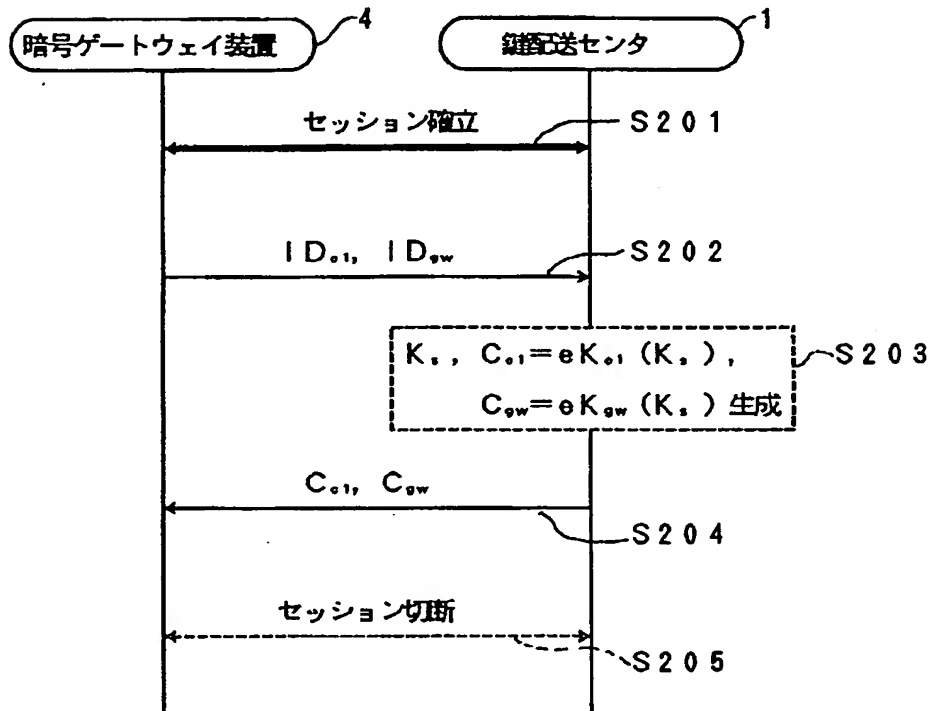
【図 8】

本発明の一実施例の鍵配送手順を示すシーケンスチャート



【図 9】

(鍵配送センター暗号ゲートウェイ装置間の鍵取得手順)



(注) $C_{s,i} = e_{K_{s,i}}(K_s)$: $C_{s,i}$ は平文 K_s を暗号鍵 $K_{s,i}$ で暗号化した結果である。

フロントページの続き

(56) 参考文献 特開 昭63-274242 (J P, A)

特開 平4-179326 (J P, A)

特開 平7-107084 (J P, A)

山口利和, 田中清人, 田辺克弘, 小柳
津育郎, LANの暗号通信における一方式,
電子情報通信学会技術研究報告 (O
F S 93-32), 日本, 社団法人電子情報
通信学会, 1994年 1月21日, Vol.
93, No. 435, p. 13-18

山口利和, 田中清人, 田辺克弘, 小柳
津育郎, LAN暗号通信方式の実装と評
価, 電子情報通信学会技術研究報告 (O
F S 93-38), 日本, 社団法人電子情報
通信学会, 1994年 3月11日, Vol.
93, No. 508, p. 7-12

山口利和, 田中清人, 田辺克弘, 小柳
津育郎, LANセキュリティ通信技術—
TCPレイヤにおける通信データの暗号
化—, NTT R&D, 日本, 社団法人
電気通信協会, 1995年 7月 8日, V
ol. 44, No. 9, pp. 653-660

(58) 調査した分野(Int. Cl. 7, DB名)

H04L 9/08

H04L 12/28